Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) ~~In a network device having a plurality of ports and providing switching functions between ports, a method for providing port security, comprising:~~ The method of claim 24, wherein using the table to control transmission of data packets through the port comprises:

receiving a ~~first~~ second data packet on [[a]] the port, the second data packet including a second source IP address and a second MAC address, the second source IP address and second MAC address forming a second source IP address and MAC address pair;

~~determining a first MAC address for the received first data packet;~~

~~determining a first source IP address for the received first data packet, wherein the first source IP address for the received first data packet and the first MAC address for the received first data packet form a first source IP address and MAC address pair;~~

comparing the ~~first~~ second source IP address and MAC address pair with ~~information in a table which stores source IP address and MAC address pairs~~ source IP address and MAC address pairs stored in the table; and

passing the ~~received first~~ second data packet through the port, when the ~~first~~ second source IP address and MAC address pair is found in the table.

2. (Canceled)

3. (Currently Amended) The method of claim [[2]] 1 further comprising:

performing a reverse IP check to confirm the learned first source IP address.

4. (Currently Amended) The method of claim 1 ~~further comprising:~~

~~determining if a second MAC address for a second received data packet is a new MAC address;~~

~~wherein when the second MAC address for the second received data packet is determined to be a new MAC address, learning the source IP address for the second MAC address, wherein the second MAC address and the learned source IP address form a second IP address and MAC address pair;~~ wherein the learning of the first source IP address utilizes at least one ~~of the processes~~ process selected from the following group of processes: (1) using a reverse address resolution protocol; (2) listening to a DHCP response packet; (3) watching for a IP header information in a data packet; and (4) listening to ARP requests and ARP reply messages~~; and~~

~~storing the second IP address and MAC address pair in the table~~.

5. (Currently Amended) The method of claim [[2]] 1 wherein the table is stored in an access control list of a content addressable memory device.

6. (Currently Amended) The method of claim 1 further comprising:

detecting when a device having a ~~second~~ third source IP address, which is stored in the table, is no longer coupled to the port; and

removing the ~~second~~ third source IP address from the table when the device having the ~~second~~ third source IP address is determined to no longer be coupled to the port.

7. (Currently Amended) The method of claim [[2]] 1 further comprising:

detecting when a device having the learned first source IP address, which is stored in the table, is no longer coupled to the port; and

removing the learned first source IP address from the table when the device having the learned first source IP address is determined to no longer be coupled to the port.

8. (Original) The method of claim 1 further comprising receiving input from a system administrator which selects a maximum number of source IP addresses which have access through a port.

9. (Original) The method of claim 1 further comprising receiving input from a system administrator which selects ports of the plurality of ports, where access though selected ports will be provided based on a source IP address and MAC address pair contained in a data packet.

10. (Canceled)

11. (Currently Amended) The method of claim 1 further comprising:

receiving a ~~second~~ third data packet on the port; and

blocking the ~~second~~ third data packet at the port, if a ~~second~~ third source IP address and a ~~second~~ third MAC address for the ~~second~~ third data packet is determined to not be stored in the table, and a maximum number of source IP addresses already have access through the port.

12. (Currently Amended) The method of claim 1 further comprising:

receiving a ~~second~~ third data packet on the port;

determining a ~~second~~ third source IP address and a ~~second~~ third MAC address for the ~~second~~ third data packet; and

storing the ~~second~~ third source IP address and the ~~second~~ third MAC address in the table, if a maximum number of source IP addresses has not already been reached for the port, and passing the ~~second~~ third data packet through the port.

13. (Currently Amended) The method of claim 12 further comprising blocking the ~~second~~ third data packet at the port, when the source IP address for the ~~second~~ third data packet is determined to not be stored in the table, and a maximum number of source IP addresses already have access through the port.

14 - 16. (Canceled)

17. (Currently Amended) A network device for use in a computer network having a plurality of hosts each host having a MAC address, the network device comprising:

a plurality of ports;

a MAC detector which operates to identify [[a]] source MAC ~~address~~ addresses for [[a]] data ~~packet~~ packets received at a first port of the plurality of ports;

a source IP address detector which operates to identify [[a]] source IP ~~address~~ addresses for [[the]] data ~~packet~~ packets received at the first port, ~~wherein the~~ a source IP address ~~for the data packet~~ and [[the]] source MAC address for [[the]] a given data packet ~~form~~ forming a source IP address and MAC address pair; and

a processor which operates to:

compare a first MAC address for a first data packet received on the first port with information in a table configured to store a plurality of source IP address and MAC address pairs;

if the first MAC address is not found in the table, learn a first source IP address of the first data packet, wherein the first MAC address and first source IP address form a first source IP address and MAC address pair, and wherein said learning is delayed from a time of receipt of the first data packet until a predetermined amount of traffic has passed through the first port;

upon learning, store the first source IP address and MAC address pair in the table;

compare [[the]] a second source IP address and MAC address pair for a second data packet received at the first port with the information in [[a]] the table ~~which stores a plurality of source IP address and MAC address pairs~~; and

pass the second data packet through the first port when the second source IP address and MAC address pair is found in the table.

18. (Currently Amended) The network device of claim 17 wherein the ~~processor~~ network device includes a content addressable memory and wherein the table is stored in an access control list of the content addressable memory.

19. (Canceled)

20. (Currently Amended) The network device of claim 17 wherein the processor further operates to block the second data packet at the first port when the second source IP address and MAC address pair is not found in the table.

21. (Previously Presented) The network device of claim 17 wherein the processor further operates to selectively block access to selected ports of the plurality of ports based on a source IP address contained in data packets received at a port.

22. (Currently Amended) ~~A method for providing port security in a network device, the method comprising:~~ The method of claim 24, wherein using the table to control transmission of packets through the port comprises:

comparing a ~~first~~ second source IP address and MAC address pair with ~~a plurality of~~ source IP address and MAC address pairs stored in [[a]] the table ~~of the network device~~, the ~~first~~ second source IP address and MAC address pair being determined from a second data packet received at [[a]] the port ~~of the network device~~;

if the ~~first~~ second source IP address and MAC address pair is found in the table, passing the second data packet through the port; and

if the ~~first~~ second source IP address and MAC address pair is not found in the table, blocking the second data packet at the port.

23. (New) The method of claim 22, wherein the network device includes a s timer configured to clear the table of one or more source IP addresses at predetermined time intervals.

24. (New) A method for providing port security in a network device, the method comprising:

receiving a first data packet on a port of the network device, the first data packet including a first MAC address and a first source IP address;

determining if the first MAC address is a new MAC address that is not included in a table of the network device, the table configured to store a plurality of source IP address and MAC address pairs;

if the first MAC address is a new MAC address, learning the first source IP address, wherein the first MAC address and the first source IP address form a first source IP address and MAC address pair, and wherein said learning is delayed from a time of receipt of the first data packet until a predetermined amount of traffic has passed through the port;

upon learning, storing the first source IP address and MAC address pair in the table; and

using the table to control transmission of data packets through the port.

25. (New) A network device for use in a computer network having a plurality of hosts, each host having a MAC address, the network device comprising:

a plurality of ports;

a table configured to store a plurality of source IP address and MAC address pairs; and

a processor configured to:

receive a data packet on the port, the data packet including a MAC address and a source IP address;

determine if the MAC address is a new MAC address that is not included in the table;

if the MAC address is a new MAC address, learn the source IP address, wherein the MAC address and the source IP address form a source IP address and MAC address pair, and wherein said learning is delayed from a time of receipt of the data packet until a predetermined amount of traffic has passed through the port;

upon learning, store the source IP address and MAC address pair in the table; and

use the table to control transmission of data packets through the port.